非接触 CPU 卡在环保排污上的应用①

夏 信[1], 王于波[1], 金学明[1], 郭 鹏[2]

[1](北京南瑞智芯微电子科技有限公司, 北京 100192)
[2](浙江环茂自控科技有限公司, 杭州 310051)

摘 要: 为确保环保排污重要数据交互、存储的安全性以及后台系统与前端总量计量设备数据传输的安全性, 本文结合现有的排污许可证制度, 提出了将国密 SM1 加密算法非接触 CPU 卡作为信息载体在环保排污上的应用模式, 并对目前在浙江省环保领域应用的具体案例进行了剖析.

关键词: 环保排污; 总量计量设备; 排污许可证; SM1 加密算法; 非接触 CPU 卡

Application of Non Contact CPU Card in the Environmental Pollution

XIA Xin[1], WANG Yu-Bo[1], JIN Xue-Ming[1], GUO Peng[2]

[1](Communication Power Utilization Technology Subcompany Beijing NARI Smartchip Microelectronics Company Limited, Beijing 100192, China)
[2](Zhejiang HuanMao Auto-Control Technology Company Limited, Hangzhou 310051, China)

Abstract: In order to guarantee the environmental protection pollution discharge important data alternately, the memory security as well as the backstage system with the front end total quantity measurement equipment data transmission security, this article unifies the existing pollution discharge permit system, proposed must contacts the country dense SM1 algorithm the non-contact CPU card to take the information carrier in environmental protection pollution discharge application pattern, and has carried on the analysis to at present in the Zhejiang Province environmental protection domain application concrete case.

Key words: environmental protection pollution discharge; total quantity measurement equipment; pollutant emission permit; SM1 encryption algorithm; non contact CPU card

智能卡技术的发展已经经历了十余年, 作为信息传输和存储的载体, 智能卡已经在金融、电信、交通、电力以及其他领域得到了广泛的应用.

在环境保护领域, 依托于排污许可证制度, 国内个别省份已经采用逻辑加密卡作为排污许可证副证, 用于排污权的购买和消费. 作为传统的信息载体, 逻辑加密卡在各领域中得到了推广和应用, 但随着 2008 年德国研究员亨里克·普洛茨(Henryk Plotz)和弗吉尼亚大学计算机科学在读博士卡尔斯滕·诺尔(Karsten Nohl)成功地破解了 Mifare 1 的安全算法, 并在互联网上公布了破解 Mifare 1 密码的方法, 逻辑加密卡的安全性成为了全球关注的焦点. 因此将逻辑加密卡作为排污权存储和交易的信息载体, 存在着极大的数据安全风险.

非接触 CPU 卡支持 ISO14443 协议, 除了具有 Mifare 1 使用便捷的优点外, 非接触 CPU 卡带有微处理器 CPU、随机存储器 RAM、只读存储器 ROM、用户数据存储区域 EEPROM、算法协处理器以及芯片操作系统等, 安全性比逻辑加密卡更高、容量比逻辑加密卡大、应用更易扩展, 从而满足了环保排污权购买、消费、数据安全以及其他相关的需求.

1 逻辑加密卡确保数据安全的方式

密钥管理是所有 IC 卡项目安全的核心, 如何确保密钥存储和使用的安全, 直接决定了数据的安全性. 逻辑加密卡在个人化写入密钥和数据时, 所有敏感的

① 收稿时间:2013-08-16;收到修改稿时间:2013-09-23

数据, 特别是各扇区的 KEYA、KEYB 都以明文的形式出现; 同时逻辑加密卡的认证原理也仅是依赖于每个扇区中独立的 KEYA 和 KEYB 的校验, 通过校验字对两组密钥进行不同的组合, 从而实现数据读写的安全控制, 但无论通过什么形式, 密钥都必须和原先预设值的固定值要相同. 因此, 逻辑加密卡在数据安全性方面存在着极大的隐患.

2 非接触CPU卡在环保排污上的应用

2.1 密码算法的选择

国密 SM1 算法是由国家密码管理局编制的一种商用密码分组标准对称算法, 分组长度和密钥长度为 128 比特, 算法不公开. 对于对称密码算法, 加密运算和解密运算使用相同的密钥, 密钥长度短, 加解密速度快, 破译难度大. 考虑到环保排污应用的实际情况, 本文推荐使用 SM1 对称算法.

2.2 非接触 CPU 卡的优势

由于各排污企业的实际应用环境比较复杂, 无论是废气还是废水排放企业的应用环境, 都有可能对卡片造成不同程度的影响, 另外, 排污信息作为系统最核心、最敏感的数据之一, 对安全的要求性较高, 因此, 排污许可证 IC 卡采用非接触形态的 CPU 卡, 主要优点如下:

(1) 非接触 CPU 卡符合 ISO/IEC 14443 规范, 能适应各种符合规范的读写机具, 通用性强;

(2) 非接触 CPU 卡安全性高于目前市面上的其他卡片;

(3) 非接触 CPU 卡操作便捷、抗干扰性好、可靠性高、具有防冲突机制.

2.3 密钥管理系统的设计

密钥管理系统是 IC 卡应用系统数据安全的核心部分, 建设符合环保排污应用的密钥管理系统, 对整个系统的数据安全起着决定性的作用.

(1) 设计思想

钥管理系统的设计是以密码技术为核心, 以智能 CPU 卡和密码设备为基础, 按照多级密钥管理体系进行设计和架构, 在确保密钥、设备以及应用安全的同时, 满足国家密码管理局对于密钥管理系统的相关标准和规范要求, 满足环保行业在省市县三级密钥管理的应用.

密钥管理系统负责密钥的产生、密钥的备份、密钥的恢复、密钥的分发、密钥的传递、密钥的删除与销毁等密钥全生命周期的管理功能. 产生的密钥用于排污许可证 IC 卡发行系统、排污许可证系统、现场服务终端总量计量设备等相关应用系统.

(2) 系统总体架构

密钥管理系统根据多级密钥体系的思想, 由上级系统生成下级系统所需的密钥, 以密码机或密钥母卡为安全载体, 采用加密保护的方式传递到下一级系统, 传递过程始终处于密文状态, 且密文不出密码机或密钥母卡, 每级母卡的使用均受传输卡的控制, 增强了密钥传输过程的安全性. 以三级密钥体系为例, 密钥下发流程框图如图 1.

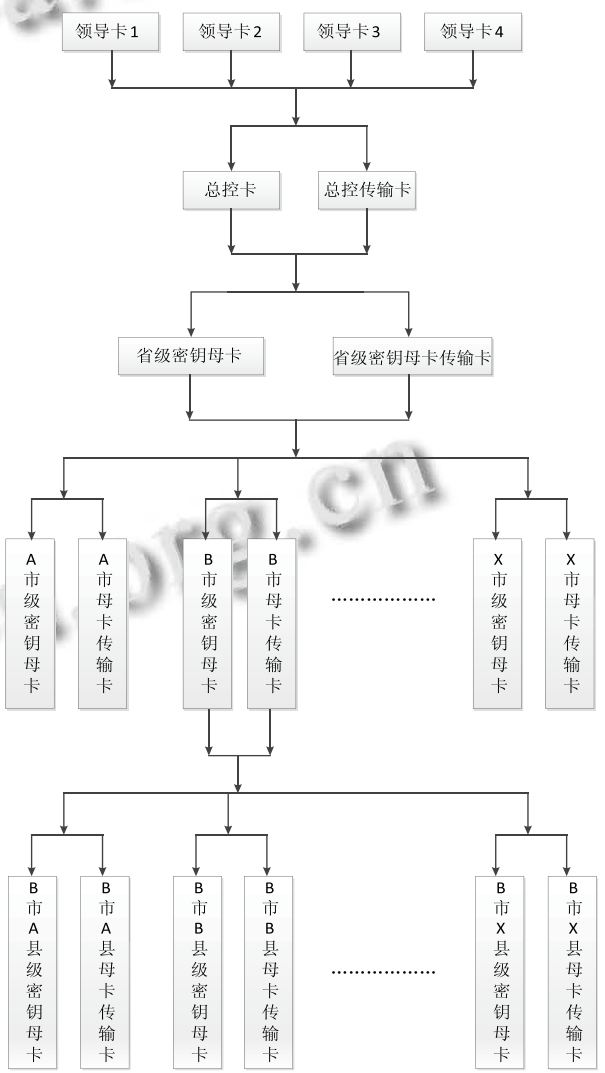

图 1 密钥下发流程框图

省级密钥管理系统为整个安全体系的最顶层系统,

负责密钥的产生、传递、备份、恢复、管理和维护功能, 同时生成根密钥, 并根据市级分散代码生成市级密钥管理系统的根密钥.

市级密钥管理系统负责省级下发密钥的接收、传递、管理与维护, 利用省级密钥管理系统下发的密码机或密钥母卡组建市级密钥管理系统, 并根据县级分散代码生成县级密钥管理系统的根密钥.

县级密钥管理系统是整个安全体系的最后一级系统, 负责上级密钥的接收、应用、管理与维护等功能, 同时产生业务应用密钥, 并通过密码机将业务密钥传递到各应用系统.

(3) 密钥的备份和恢复

根密钥和领导分散因子备份和恢复均采用门限机制, 密钥在备份时, 将密钥数据按照门限机制算法进行分割, 得到 5 份密钥, 并将这 5 份密钥分别备份到 5 张密钥母卡中, 在需要密钥还原时, 从 5 张备份的母卡中任取 3 张, 即可对密钥数据进行还原. 门限机制增强了密钥的安全性, 同时也对系统的管理带来了便捷.

(4) 系统的三权分立

密钥管理系统采用三权分立机制, 实现对系统管理员的统一管理, 确保系统自身安全. 三权包括系统管理员、安全员、审计员, 三权之间相互制约、相互独立. 系统管理员可定义并产生操作员及操作员可执行的权限, 安全员对操作员进行启/禁用授权操作, 未授权的操作员无法正常工作. 通过对系统设置三员, 并为每个角色配置安全登陆 Key, 从管理的角度, 加入安全控制手段, 确保系统使用的安全性.

(5) 系统的部署

以三级密钥管理系统为例, 一级密钥管理系统部署在省级环保厅机房, 二级密钥管理系统部署在市级环保局机房, 三级密钥管理系统部署在区县级环保局机房.

2.4 环保排污应用卡片用途及卡片发行

根据实际的应用和管理需求, 卡片种类一般包括排污许可证 IC 卡、运维卡、管理卡以及现场参数设置卡, 具体用途如下:

排污许可证 IC 卡: 作为排污许可证副证, 用于存放排污许可证的相关信息, 可进行排污权的购买和使用, 由企业用户持有.

运维卡: 存放运维人员基础信息, 实现监督签到功能, 由环保运维人员持有.

管理卡: 用于激活或停用企业端安装的排污总量计量设备, 由环保监管部门持有.

现场参数设置卡: 用于对已经激活使用的排污总量计量设备进行参数设置.

所有的卡片初次发行均在省环保厅进行, 建立对应应用的文件结构, 同时灌装省级发行密钥. 地市级和县级环保部门在省环保厅领取各类卡片后, 需要在本地业务系统进行二次发行并更新对应的本地业务密钥, 同时写入相关信息.

2.5 浙江省环保领域应用案例

浙江省环保厅依托安全可靠的三级密钥管理体系建设, 实现了不同区域排污权的独立管理、购买和交易, 并采用排污许可证 IC 卡电子证照模式, 建立了一套企业环保身份验证体系, 实现刷卡排污与排污许可证相结合的应用, 将排污企业的排污许可证信息通过电子证件形式进行管理, 通过该 IC 电子证照作为企业的排污许可证副证, 记录企业的相关排污总量信息, 做到“一企一证一卡”.

排污许可证 IC 卡电子证照是污染源企业的合法身份证, 是环保职能部门对污染源企业进行环境管理的信息媒介, 是环保职能部门规范行业行为、规范环境管理的手段. 作为区域推行刷卡排污的信息媒介存在, 通过该 IC 卡以企业为视角汇聚现有的环保业务信息, 实现“凭卡申报、超标报警、企业申请、环保批准”的模式, 同时也为其他环境管理手段, 例如: 排污费收取、企业现场巡检、行政执法提供了控制手段, 从而借助技术手段实现污染的有效控制和环境的有效保护.

2.5.1 排污许可证管理系统总体逻辑架构图

浙江省环保排污许可证系统属于新建设系统, 使用现阶段浙江省环保厅建设中的地理信息系统的地图服务, 并将许可证数据通过数据交换平台提供给省环保厅数据中心、一厂一档、排污权交易、行政执法等系统应用, 地市系统所需许可证数据也通过数据交换平台下发. 系统逻辑架构图如图 2.

2.5.2 应用实例

萧山经济技术开发区热电有限公司目前总装机容量为 3 台 75T/H 循环流化床锅炉和 2 台 12MW 抽凝式发电机组, 年发电能力 1.56 亿 KWH、供热能力 200 万吉焦. 本次试点中选择萧山热电总排放口进行总量监管.

通过试点建设, 在污染物总排放口部署刷卡排污总量计量设备, 用于排污许可证 IC 卡刷卡实现排污权

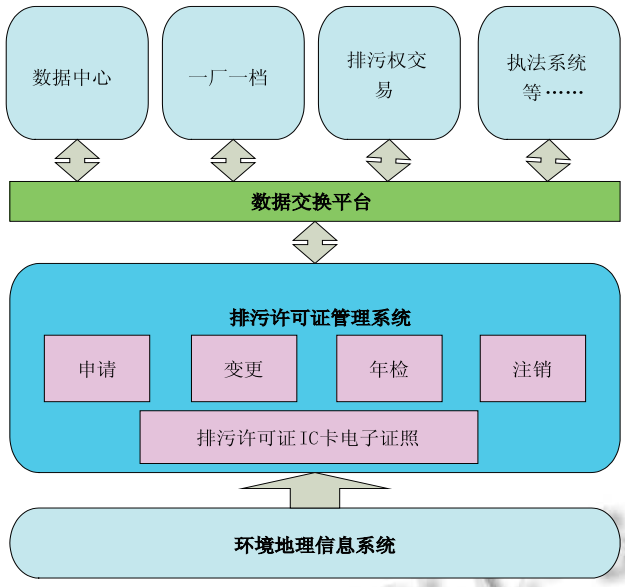

图 2 系统逻辑架构图

增加、污染物排放的监测和控制. 同时在省环保厅信息中心机房部署企业排污总量监管系统平台和环保专用密码机, 用于监控和管理试点企业污染物总量排放数据、实现设备和系统平台间数据的安全传输, 系统结构图如图 3.

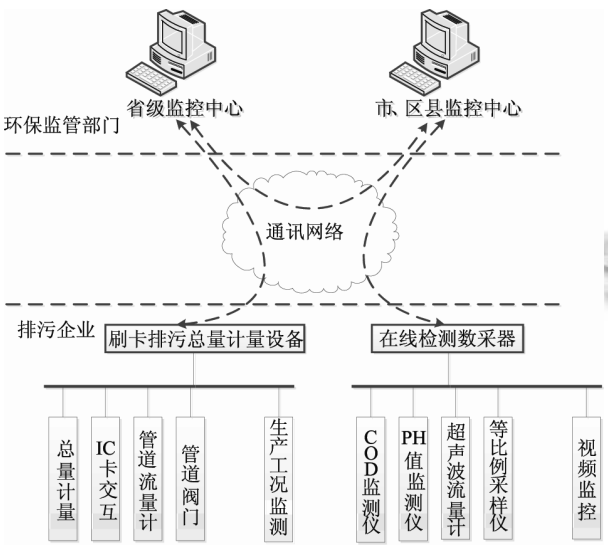

图 3 系统结构图

目前试点企业排污总量计量设备和省环保厅排污总量监管系统平台开始运行, 已经实现试点企业总量排放数据的 24 小时监测, 主要监测废气、二氧化硫、氮氧化物排放总量的 10 分钟数据和小时数据, 并以此进行企业排放总量计算, 对照监测机组负荷、脱硫效率、脱硝效率等企业生产过程工况数据, 同时通过总量计量设备内置安全模块, 对监测数据等敏感信息进行加密并上传省中心平台, 通过平台环保专用密码机进行解密, 获取相关数据, 以防止重要环保数据外泄, 造成社会的不良影响.

刷卡排污总量控制是排污许可证制度的延伸, 项目试点以排污许可证总量核准数据为依据, 以刷卡排污为手段, 以控制排污总量和污染减排为目的, 实现总量计量与环境执法联动, 体现环境资源有限性和有价性, 促进企业真正落实保护和改善环境质量的目标.

2.5.3 试点项目中非接触 CPU 卡应用遵循以下建设思路

1) 部署在废气污染源的刷卡排污总量控制系统以在线监测数据为总量计算依据, 以实时定量监测为目标, 对企业排放总量进行计量.

2) 环保厅排污权交易平台和排污监测平台采用环保专用密码机, 总量计量设备嵌入 SM1 算法安全模块, 企业排污管理采用非接触 CPU 卡, 确保环保敏感信息安全传递.

3) 实现刷卡排污与排污许可证相结合, 排污企业可持卡到环保政务大厅进行排污权购买, 当企业进行“刷卡”操作时, 直接使用排污许可证 IC 卡电子证照进行, 实现企业环保业务的电子化、一体化管理.

4) 对于排放量达到允许排放量 90%的企业发送提醒; 对于已超量排放的企业通过总量控制系统发出警报, 并及时通知环境监察执法部门进行查处, 环境监察执法部门可以通过管理卡和现场参数设置卡, 对排污总量计量设备进行控制和参数修改, 实现总量计量与环境执法联动.

5) 环保厅运维人员持运维卡对排污企业进行巡检, 实现签到功能.

整个系统的建设, 为环保监管部门定量掌握污染源企业污染物排放数据提供技术支撑, 为管理部门促进排污许可证和排污权交易工作的稳步推进、对有效监管排污行为提供强有力的管理手段.

3 结语

密码技术和非接触 CPU 卡在各行各业已经得到了广泛的应用, 比如市政公交一卡通、校园卡以及其他公共事业领域, 非接触 CPU 卡作为重要的信息载体, 安全性和便捷性在实际的使用中已经得到了

(下转第 204 页)

tlp_type=1000000b 为存储器写, 数据负载长度为 10H, 并生成 16 个写使能脉冲 wr_en_o 将数据存储到 block ram, 在检测到 m_axis_rx_tlast 高电平时, 该 TLP 接收结束. 图 6 为发送模块发送 TLP 时序图, 首先数据处理模块将 TLP 发送请求 req_tx_tlp 置有效, 触发 req_wr_i 生成一个高脉冲; 然后发送模块开始发送生成填充该 TLP 头标, 接着依次将要发送 TLP 有效数据, 在发送即将结束时, s_axis_tx_tlast 产生一个高脉冲, 告之 PCIE 核本帧报文发送完成.

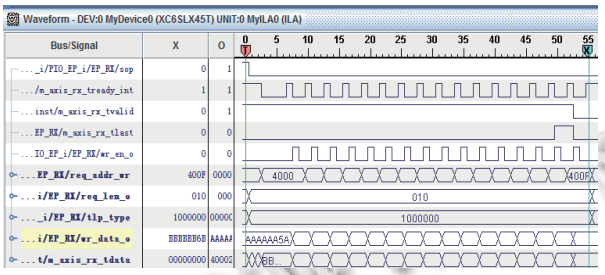

图 5　TLP 接收时序图

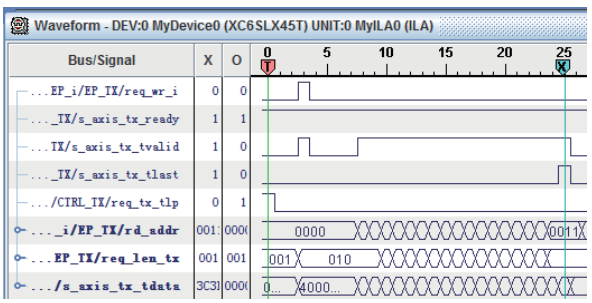

图 6　TLP 发送时序图

4　结语

本文应用 PCI Express 技术, 使用 FPGA 设计实现了一种点对点以太网数据传输的解决方案, 并充分使用 spartan-6 架构 FPGA 内部资源, 降低了系统开发的难度. 此方案已广泛用于实际应用中, 提供了高带宽及高可靠性数据传输, 解决了传统使用并行总线数据吞吐量不足的问题, 具有极大提升了智能变电站数据传输的性能.

参考文献

1 Q/GDW 383.智能变电站技术导则.北京:国家电网公司, 2009.
2 Xilinx. Spartan-6 FPGA Integrated Endpoint Block for PCI Express Pre-Production User Guide. 2010.
3 王齐.PCI Express 体系结构导读.北京:机械工业出版社, 2010.3:101–228.
4 王伟,傅其祥.基于 PCIe 总线的超高速信号采集卡的设计.电子设计工程,2010,18(5):43–45.

(上接第 227 页)

充分的体现. 本文提出的基于非接触 CPU 卡的排污许可证系统安全体系, 实现了从排污许可证系统到企业端的排污总量计量设备的数据交互安全以及非接触 CPU 卡与排污许可证系统、排污总量计量设备的交互安全, 确保了环保敏感数据的准确性、安全性、保密性, 符合环保应用对信息安全的需求, 为政府节能减排提供了强有力的技术支撑.

参考文献

1 哈力曼• 哈麦拉,田义文.我国污染物总量控制制度研究.我国污染物总量控制制度研究.安徽农业科学, 2013,41(5):2237-2238.
2 宋国君,韩冬梅,王军霞.中国水排污许可证制度的定位及改革建议.环境科学研究,2012,25(9):1071-1076.
3 孙俊峰.浅谈中国排污许可证制度.环境科学导刊,2011,30(5).
4 闫海超,张俊,李成思.小小 IC 卡卡住排污量.中国环境报,2011-04-04(003).
5 马利艳.水污染物排放许可证制度探讨.学理论,2012, 14:132-02.